I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system in accordance with 37 CFR §1.6 (a)(4).

Dated: June 22, 2010 Signature: _____
Sanro Clobes, Reg No. 52,535

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	U.S. Patent Application of Tet Hin YEAP *et al.*		
Appl. No.:	10/673,509	Art Unit:	2455
Filed:	September 30, 2003	Examiner:	Shawki Saif ISMAIL
For:	SYSTEM AND METHOD FOR SECURE ACCESS		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MAIL STOP AF
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Commissioner:

Kindly consider the following remarks / arguments forming part of the present Pre-Appeal Brief Request for Review.

As will be shown below, it is respectfully submitted that independent claims 35, 45, 67 and 68 were improperly rejected in light of an admitted absence of basis for rejection and/or reliance on improper or inexistent Official Notice and/or reliance on Official Notice where not appropriate. Furthermore it is respectfully submitted that the Examiner has omitted one or more essential elements needed for a prima facie rejection, and that these claims clearly comprise features not disclosed or rendered obvious by the cited reference(s) including U.S. Patent no. 7,395,549 (Perlman). Moreover, the dependent claims, by virtue of their respective dependencies, also include features that are not met by the cited references.

I. Rejection of Claims 35 and 68 is defective because it fails to identify new grounds of rejection

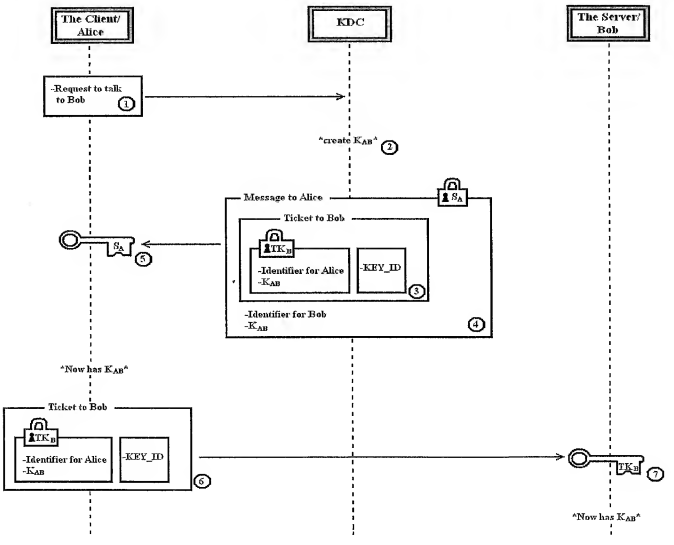
In the Applicant's response to the Office Action of February 3, 2009 (response sent May 14, 2009) claim 35 was amended in order to introduce therein the subject matter of former dependent claim 42 which was cancelled. A similar amendment was made to claim 68 and remarks were made to address the Examiner's rejection of claims 35 and 68, which took into account the Examiner's position with respect to former dependent claim 42.

In the current Office Action, the Examiner states on page 2 that "Applicants (*sic*) arguments have been fully considered and are persuasive, however upon further review and consideration a new

grounds of rejection is hereby made" (emphasis added). The Examiner also states on page 5 of the Office Action that "Applicants' arguments have been fully considered however they are deemed moot in view of the new ground(s) of rejection" (emphasis added). However, in the rejection of claims 35 and 68, the Examiner provides no such "new grounds of rejection". Rather, regarding claim 35, the Examiner repeats portions of the arguments previously made in respect of former claim 35, and merely cites a passage of Perlman which, it is remarked, was already previously cited against former claim 42 and dealt with in the previous response. Regarding claim 68, the Examiner merely states that this claim "[does] not teach or define any new limitations beyond the claims above, therefore, [it] is rejected for similar reasons." Since no "new grounds of rejection" have been identified and since the Examiner considers the previously submitted arguments to have been "persuasive", it is respectfully submitted that the current rejection of claims 35 and 68 is defective and cannot stand.

II. Rejection of Claims 35 and 68 omits essential elements for prima facie case of anticipation

It is respectfully submitted that the Examiner has clearly omitted at least one element required to establish a prima facie rejection of claims 35 and 68. In particular, certain elements of the claims are clearly missing from the cited art.



Perlman relates to providing a key distribution center while avoiding storing long-term server secrets. In particular, a client (Alice) and a server (Bob) make use of a key distribution center (KDC) to permit communication between each other. To communicate with Bob, Alice sends a request to the KDC. The KDC then "creates a session key, K_{AB}, to be used in communications between Alice and Bob. KDC 102 retrieves Bob's temporary secret key, TK_B, and then creates a "ticket to Bob" by using TK_B to encrypt the identifier for "Alice" and K_{AB}, and by attaching the key identifier for TK_B, KEY_ID, in the clear" (col. 6, lines 56-61).

The method of establishing communication between Alice and Bob is illustrated in the included Figure. As shown, communication is initiated by the client/Alice by sending the KDC a request ①, to talk to the server/Bob (col. 6, ln. 56-61). Upon receiving this request, at ②, the KDC creates K_{AB}, an encryption key that is to be used for communication between Alice and Bob (col. 6, ln. 56-58). The KDC then generates a ticket to Bob ③, which comprises an Identifier for Alice and K_{AB}, both encrypted with TK_B, and a KEY_ID indicative of TK_B (col. 6, ln. 58-61). The KDC then generates a Message to Alice ④, which comprises the ticket to Bob as well as an Identifier for Bob and (unencrypted) K_{AB} (col. 6, ln. 62-65). The Message to Alice is encrypted using S_A, which is a function of Alice's password and sent to Alice. Upon reception of the Message to Alice, the client/Alice decrypts ⑤, the Message to Alice using S_A and derives the Identifier for Bob, K_{AB} and the Ticket to Bob (col. 6, ln. 66-67). The client/Alice now has K_{AB}. Alice then sends ⑥, the Ticket to Bob to the server/Bob (col. 7, ln. 5-6) who decrypts ⑦ the Ticket to Bob using TK_B (col. 7, ln. 8-9). Bob now also has K_{AB}. Alice can now prove it also knows K_{AB} and encrypted communication can take place between Bob and Alice.

Thus, one can make the following observations regarding Perlman:

A) The session key, K_{AB}, is necessarily delivered to the client/Alice before it can be delivered to the server/Bob, since the client/Alice is responsible for delivering it (within the Ticket to Bob) to the server/Bob.

B) No authentication server ever sends an encryption key for communication between Alice and Bob to the server/Bob. Rather, the KDC sends two copies of K_{AB} to the client/Alice (one of which is within the Ticket to Bob) and the client/Alice is responsible for transmitting the K_{AB} (within the Ticket to Bob) to the server/Bob. In fact no one entity sends two keys (or even one same key) to two different recipients.

C) The same session key K_{AB} is used by both the client/Alice and the server/Bob for communication therebetween. There are no complementary keys.

D) No two entities communicate together using two complementary keys. Alice and Bob, communicate using K_{AB} alone.

Perlman can therefore not be held to teach delivery from an authentication server of a first key to a client and a second key to an access controller. Perlman's failure to teach such a delivery also implies that the delivery will fail to provide the second key complementary to the first key. And it also follows that there is no such delivery wherein the first key is delivered to the client only after the second key has been successfully delivered to the access controller.

The Applicant would also like to address an apparent misinterpretation of Perlman by the Examiner. In alleging that "said access controller [...] operable to deliver a first key to said client and

a second key to said controller" is disclosed by Perlman, the Examiner cites not only sections of Perlman describing dissemination of K_{AB} but also a section of Perlman that describes the establishment of a temporary secret key TK_B for the server/Bob. It thus appears that the Examiner interprets TK_B and K_{AB} as a set of a first and second key delivered respectively to a client and an access controller by an authentication server, and complementary to one another, and used for communications between a client and an access controller when they are connected. However, it will be appreciated that a) TK_B and K_{AB} are not delivered by the same entity (authentication server or otherwise – K_{AB} is delivered by the KDC to the client/Alice, while the TK_B is created by the server/Bob and delivered to the KDC); b) TK_B is not complementary to K_{AB}; and c) TK_B is not used to encrypt communication from Alice to Bob or *vice versa*. Thus it would be incorrect to interpret TK_B and K_{AB} as the first and second keys recited in claim 35.

Thus, Perlman completely fails to disclose "an authentication server operable to communicate with said client and said access controller via a second communication medium and further **operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key** such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys", "wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met" and "said first key is delivered to said client only after said second key has been successfully delivered to said access controller". It is therefore respectfully submitted that the Examiner's rejection clearly omits at least one element required to establish a prima facie case of anticipation.

III. Rejection of Claims 45 and 67 is defective due to improper Official Notice

It is respectfully submitted that the Examiner's rejection is defective due to inappropriate usage of the Official Notice paradigm. In particular, the Examiner states "Official Notice teaches the use of three way handshaking protocol in a PKI system to verify the client's integrity". However, it is improper to suggest that an Official Notice "teaches" anything. Rather, Official Notice should be taken of a fact that is considered to be well known or part of the common general knowledge in the art, and capable of such instant and unquestionable demonstration as to defy dispute (*In Re Ahlert* 165 USPQ 418). It follows that an Official Notice should not teach anything new. In the Office Action, the Examiner never actually takes notice that three way handshaking protocols are known, and therefore relies on an improper or inexistent Official Notice.

[1] Notwithstanding the above, even if a hypothetical reference did teach that the use of three way handshaking protocol in a PKI system to verify the client's integrity were known, the combination of the fictitious reference and Perlman would still not teach anything related to the generation of a random number. Three way handshaking does not in any way imply random number generation, nor does Perlman pertain to random number generation at all. Random numbers are not disclosed in Perlman, whether in the creation of the session key K_{AB} (which is created by the KDC and sent to Alice), the temporary secret key TK_B (which is created by the server/Bob and sent to the KDC) or S_A (which is a function of Alice's password). It therefore follows that the hypothetical combination Perlman and a fictitious "three way handshaking" reference would not teach anything related to

a) encrypting a random number using a first key;
b) delivering a random number from a client to an access controller;
c) delivering an encrypted random number from the client to the access controller;
d) decrypting the encrypted random number by the access controller using a second key (there is also no "first" and "second" complementary keys in Perlman, as discussed above);
e) comparing the random number and the decrypted version of the encrypted random number; or
f) a decision to pass at least a portion of an instruction (received from the client) if the comparison finds a match.

Furthermore, it is respectfully submitted that the Examiner cannot take Official Notice that "the use of three way handshaking protocol in a PKI system to verify the client's integrity" is known without an explicitly set forth basis for such reasoning (M.P.E.P. 2144.03) of which none was provided. Moreover, it is respectfully submitted that any assertion of technical facts should be supported by references (ibid). For the above reasons, it is respectfully submitted that the rejection based on Official Notice is improper.

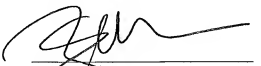
IV. Rejection of Claims 45 and 67 omits essential elements for prima facie case of obviousness

It is respectfully submitted that the Examiner did not argue the subject matter of the claims, and completely failed to address any of "a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found" recited in claim 45. Rather, the Examiner admits that Perlman fails to teach these features but mere states that "it would be obvious [...] to incorporate the teachings of Official Notice into the system or Perlman in order to allow the server to verify the client's integrity". Given that nowhere does the alleged "Official Notice" relate to random numbers or any of the above features of claim 45, it should be readily apparent that the Examiner has not at all established that claims 45 and 67 are obvious, but that the rejection is defective for having omitted at least one element required to establish prima facie obviousness.[1]

III - CONCLUSION

In conclusion, it is believed that claims 1-3, 5, 13-24, 26, 34-42, 52, 54-106, and 108 are in condition for allowance, and the Notice of Allowance is earnestly and respectfully solicited.

Respectfully submitted,



Dated: June 22, 2010

Samo Zlobec
Reg. No. 52,535
Agent for the Applicants

SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA

Telephone: (514) 954-1500
Facsimile: (514) 954-1396